

ALERTE - Faux ordres de virements internationaux (FOVI) -

Les escroqueries aux faux ordres de virement (FOVI) consistent, au moyen de manoeuvres frauduleuses, à obtenir de la part d'une entreprise un virement bancaire indu sur des comptes ouverts à l'étranger.

Dans les Landes depuis janvier 2016, trois entreprises se sont ainsi faites escroquer par le biais d'un FOVI. Le montant du préjudice est particulièrement élevé (de l'ordre de 300 000 euros pour l'une d'elle).

Quelques règles simples

Pour s'en prémunir, les entreprises peuvent mettre en place un ensemble de mesures simples de sécurité pour décourager les escrocs.

- ⑩ **Rappeler à l'ensemble des collaborateurs** la nécessité d'avoir un usage prudent des réseaux sociaux privés et professionnels. Les alerter sur l'importance de ne pas y divulguer d'informations concernant le fonctionnement de l'entreprise.
- ⑩ Sensibiliser **régulièrement l'ensemble des employés des services comptables, trésorerie, secrétariats, standards**, de ce type d'escroquerie. Prendre l'habitude d'en informer systématiquement les **remplaçants** sur ces postes.
- ⑩ **Instaurer des procédures de vérifications** et de signatures multiples pour les paiements internationaux.
- ⑩ Rompre la chaîne des mails pour les courriers se rapportant à des virements internationaux en **saisissant soi-même l'adresse habituelle du donneur d'ordre**.
- ⑩ Maintenir à jour le système de sécurité informatique.
- ⑩ Accentuer la vigilance sur les **périodes de congés scolaires**, les **jours fériés** et les **jours de paiement des loyers**.

Reconnaître les signes d'une attaque

- ⑩ Une **demande de virement à l'international, non planifiée**, au caractère **urgent** et **confidentiel** : dans ce cas, contacter son interlocuteur habituel avec les coordonnées connues de la société.
- ⑩ **Se méfier de tout changement de coordonnées téléphoniques ou mails**. Attention, la communication d'un nouveau numéro à l'indicatif français n'est pas une garantie.
- ⑩ **Se méfier d'un contact direct d'un escroc se faisant passer pour un membre de la société ou un responsable qui va faire usage de flatterie ou de menace dans le but de manipuler son interlocuteur**.
- ⑩ Pour asseoir sa crédibilité et usurper une fonction, l'escroc apportera une abondance de détails sur l'entreprise et son environnement : données personnelles concernant le chef d'entreprise, ses collaborateurs...

En cas de doute, prendre attache directement avec la personne au sein de la société, soit physiquement soit avec les coordonnées connues de l'entreprise.

Que faire en cas d'attaque ?

- ⑩ Demander immédiatement à la banque le retour des fonds
- ⑩ **Déposer une plainte** auprès des services de police et de gendarmerie, en apportant un maximum d'éléments. Un dépôt de plainte rapide permet d'optimiser les chances de récupérer les fonds escroqués.